AMENDMENTS TO THE CLAIMS

The following listing of claims replaces all prior versions of the claims and all prior listings of the claims in the present application.

1. (withdrawn) A multiple modulus selector, comprising:

a modulus recoder for receiving a n-bit modulus number M and a previous sum and current partial product, and for producing a selection signal; and

a multiplexer for receiving four inputs -M, 0, M, and 2M, and for selecting one of the inputs based on the selection signal.

2. (withdrawn) The multiple modulus selector of claim 1, wherein the input -M is obtained by inverting the modulus number M.

3. (withdrawn) The multiple modulus selector of claim 1, wherein the input 2M is obtained by shifting the modulus number M.

4. (withdrawn) The multiple modulus selector of claim 1, wherein the modulus number M is stored in a register.

5. (withdrawn) The multiple modulus selector of claim 1, wherein the modulus recoder further produces a multiple modulus negation indicating signal, and

wherein the multiple modulus negation indicating signal is input to an accumulator.

6. (withdrawn) The multiple modulus selector of claim 1, wherein the n-bit modulus number M includes a next-least-significant bit, and

wherein the previous sum and current partial product is a two-bit number, including a least-significant bit and a next-least-significant bit.

7. (withdrawn) The multiple modulus selector of claim 1, wherein the selection signal includes two bits.

8. (currently amended) An accumulator for accelerating speed of a Montgomery modular multiplier, for reducing power consumption of a Montgomery modular multiplier, or for accelerating the speed of and reducing the power consumption of a Montgomery modular multiplier in a cryptosystem, the accumulator comprising:

a plurality of compressors adapted to operate in a carry save mode, each of the compressors receiving a multiple modulus, a partial product, a

corresponding current sum, and a corresponding current carry, and adapted to produce a corresponding next sum and a corresponding next carry;

a sum register adapted to receive the corresponding next sum from respective compressors, and adapted to output a corresponding updated current sum; and

a carry register adapted to receive the corresponding next carry from the respective compressors, and adapted to output a corresponding updated current carry.

9. (previously presented) The accumulator of claim 8, wherein the sum register and the carry register are separate registers.

10. (original) The accumulator of claim 8, wherein the multiple modulus is produced from a modulus.

11. (previously presented) The accumulator of claim 10, wherein n is the bit length of the modulus, and

wherein the plurality of compressors include n+3 compressors.

12. (original) The accumulator of claim 11, wherein the modulus is stored in an n-bit register.

13. (original) The accumulator of claim 8, wherein the partial product is produced from a multiplicand and a multiplicator.

14. (original) The accumulator of claim 13, wherein n+1 is the bit length of the multiplicand.

15. (original) The accumulator of claim 14, wherein the multiplicand is stored in an (n+1)-bit register.

16. (previously presented) The accumulator of claim 13, wherein if n is even, then n+2 is the bit length of the multiplicator, and

wherein if n is odd, then n+1 is the bit length of the multiplicator.

17. (previously presented) The accumulator of claim 16, wherein if n is even, the multiplicator is stored in an (n+2)-bit register, and

wherein if n is odd, the multiplicator is stored in an (n+1)-bit register.

18. (original) The accumulator of claim 8, wherein each of the plurality of compressors is a 5:2 compressor.

19. (previously presented) The accumulator of claim 8, wherein a first group of the plurality of compressors further receives a compensating word to produce the corresponding next sum and the corresponding next carry.

20. (currently amended) The accumulator of claim 19, wherein the compressors of the first group ~~of the plurality of compressors~~ are [[full]] a first compressor[[s]], respectively.

21. (original) The accumulator of claim 19, wherein a second group of the plurality of compressors does not receive the compensating word.

22. (currently amended) The accumulator of claim 21, wherein the compressors of the second group ~~of the plurality of compressors~~ are ~~reduced~~ a second compressor[[s]], respectively.

23. (previously presented) The accumulator of claim 8, wherein n+2 is the bit length of the partial product, and

wherein n+2 is the bit length of the multiple modulus.

24. (previously presented) The accumulator of claim 19, wherein 2 is the bit length of the compensating word.

25. (currently amended) The accumulator of claim 20, wherein the [[full]] first compressors include three full adders.

26. (currently amended) The accumulator of claim 22, wherein the ~~reduced~~ second compressors include one half adder and two full adders.

27. (previously presented) The accumulator of claim 8, further comprising:

a carry propagate adder for receiving a finally updated current sum and a finally updated current carry, and for outputting a final sum in normal number representation; and

a final register for storing the final sum.

28. (original) The accumulator of claim 8, wherein the plurality of compressors operate in both the carry save mode and a carry propagate mode.

29. (previously presented) The accumulator of claim 28, wherein the carry save mode and the carry propagate mode are determined by a control signal.

30. (previously presented) The accumulator of claim 28, wherein a first group of the plurality of compressors further receives a compensating word to produce the corresponding next sum and the corresponding next carry.

31. (original) The accumulator of claim 30, wherein the first group of the plurality of compressors are full compressors.

32. (original) The accumulator of claim 30, wherein a second group of the plurality of compressors does not receive the compensating word.

33. (original) The accumulator of claim 32, wherein the second group of the plurality of compressors are reduced reconfigurable compressors.

34. (original) The accumulator of claim 33, wherein each of the reduced reconfigurable compressors includes:

a multiplexer group for reconfiguring each of the reduced reconfigurable compressors to operate in both the carry save mode and the carry propagate mode.

35. (original) The accumulator of claim 34, wherein each multiplexer group includes three 2:1 multiplexers.

36. (previously presented) The accumulator of claim 33, wherein each of the reduced reconfigurable compressors includes:

a multiplexer group that reconfigures the reduced reconfigurable compressor to operate in either the carry save mode or the carry propagate mode according to a control signal.

37. (previously presented) The accumulator of claim 36, wherein the carry save mode includes:

a first signal flowing from a middle full adder of a current compressor to a bottom full adder of the current compressor;

a second signal flowing from a top adder of a lower compressor to the bottom full adder of the current compressor; and

a third signal flowing from a middle full adder of the lower compressor to the bottom full adder of the current compressor.

38. (previously presented) The accumulator of claim 36, wherein the carry propagate mode includes:

a first signal flowing from a bottom full adder of a lower compressor to the multiplexer group of a higher compressor; and

a second signal flowing from the multiplexer group of the higher compressor to a bottom full adder of the higher compressor.

39. (previously presented) The accumulator of claim 33, wherein each of the reduced reconfigurable compressors includes:

a multiplexer group for receiving a sum of a middle full adder of a current compressor, a corresponding updated current carry of a lower compressor, a first and second secondary output of the lower compressor, a corresponding updated current sum of the current compressor, and the corresponding next carry of the lower compressor, and for outputting first through third outputs.

40. (previously presented) The accumulator of claim 31, wherein the full compressors include three full adders.

41. (previously presented) The accumulator of claim 33, wherein the reduced reconfigurable compressors include one half adder, two full adders, and three 2:1 multiplexers.

42. (withdrawn) A Montgomery multiplier, comprising:

a multiple modulus selector, wherein the selector selects a multiple modulus from one of -M, 0, M, and 2M, where M is an n-bit modulus number;

a Booth recoder, wherein the Booth recoder provides first values used to obtain a partial product value; and

an accumulator, wherein the accumulator accumulates second values obtaining a result for the Montgomery multiplier.

43. (withdrawn) The Montgomery multiplier of claim 42, further comprising:

a modulus number register, wherein the modulus number register holds a modulus value;

a multiplicand register, wherein the multiplicand register holds a multiplicand value;

a multiplier register, wherein the multiplier register holds a multiplier value;

an AND gate, where the AND gate combines two values derived from the multiplicand value and the multiplier value; and

two adders;

wherein the adders combine values from the accumulator and the AND gate to produce a combined value, and

wherein the multiple modulus selector inputs the combined value.

44. (withdrawn) A method of multiple modulus generation, comprising:

receiving a modulus;

receiving a previous sum and current partial product, wherein the modulus and the previous sum and current partial product are used to produce multiple modulus values of -M, 0, M, and 2M.

45. (withdrawn) The method of claim 44, further comprising:

receiving only a portion of the modulus, the portion being the second-least-significant bit of the modulus.

46. (withdrawn) The method of claim 44, further comprising:

receiving only a portion of the previous sum and current partial product, the portion being the two least-significant bits of the previous sum and current partial product.

47. (withdrawn) The method of claim 44, further producing:

a selection signal;

wherein the selection signal is used to select a value of the produced multiple modulus values.

48. (withdrawn) The method of claim 47, further producing:

a multiple modulus negation indicating signal;

wherein the multiple modulus negation indicating signal is used to produce a complement of the selected value.

49. (withdrawn) A method of partial product generation, comprising:

receiving a multiplier number; and

generating a partial product selection signal, a partial product enabling signal, and a partial product negation indicating signal to produce at least one partial product value.

50. (withdrawn) The method of claim 49, further comprising:

shifting the multiplier number by two bits.

51. (currently amended) A method of accumulating for accelerating speed of a Montgomery modular multiplier, for reducing power consumption of a Montgomery modular multiplier, or for accelerating the speed of and reducing the power consumption of a Montgomery modular multiplier in a cryptosystem, the method comprising:

receiving a plurality of multiple moduli, partial products, corresponding current sums, and corresponding current carries to produce a corresponding next sum and next carry;

generating updated current sums and updated current carries;

iterating the receiving and the generating until a multiplier operand is consumed to generate a result in redundant representation; and

performing carry propagation addition to generate a result in normal representation.

52. (previously presented) The method of claim 51, wherein the iterating is carry save addition performed by a carry save adder.

53. (previously presented) The method of claim 51, wherein the carry propagation addition is performed by a carry propagation adder.

54. (previously presented) The method of claim 53, further comprising:

generating a switching signal.

55. (previously presented) The method of claim 54, further comprising:

switching between carry save addition and the carry propagation addition using the switching signal.

56. (withdrawn) A method of performing radix 2^N Montgomery multiplication, where N>1, comprising;

receiving a multiplicand, a modulus, and a multiplier;

performing carry save addition on a plurality of inputs related to the multiplicand, modulus, and multiplier to generate a result in redundant representation; and

performing carry propagation addition to generate a result in normal representation.

57. (withdrawn) The method of claim 56, wherein the carry save addition is performed by a carry save adder, and

wherein the carry propagation addition is performed by a carry propagation adder.

58. (withdrawn) The method of claim 56, wherein the carry save addition is performed by an accumulator, and

wherein the carry propagation addition is performed by the accumulator.

59. (withdrawn) The method of claim 56, further comprising:

generating a switching signal.

60. (withdrawn) The method of claim 59, further comprising:

switching between the carry save addition and the carry propagation addition using the switching signal.

61. (withdrawn) A method of performing radix 2^N Montgomery multiplication, where N>1, comprising:

receiving a multiplicand, a modulus, and a multiplier;

performing accumulation in a carry save mode on a plurality of inputs related to the multiplicand, modulus, and multiplier to generate a result in redundant representation; and

performing conversion in carry propagation mode on the result in redundant representation to generate a result in normal representation.